(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－153956

(43)公開日　平成10年(1998)６月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
			６４０Ｄ
			６４０Ｚ
	６２０		６２０Ａ
			６２０Ｚ

審査請求　未請求　請求項の数11　ＯＬ　（全 18 頁）

(21)出願番号　特願平9－261762

(22)出願日　平成９年(1997)９月26日

(31)優先権主張番号　特願平8－256945

(32)優先日　平８(1996)９月27日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　新保　淳
東京都府中市東芝町１番地　株式会社東芝府中工場内

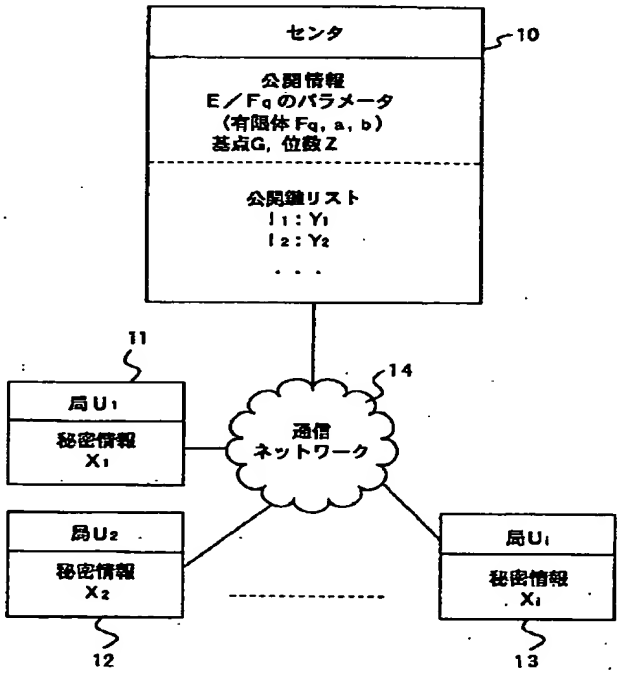
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　電子署名方法、電子署名システム及び、記録媒体

(57)【要約】

【課題】様々な運用形態を考慮した多重署名システムを容易に構成できる電子署名方法を提供する。

【解決手段】有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、その上の基点Ｇとを含むシステム情報と、楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを用いて、任意に生成された乱数ｋと楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する点Ｒの少なくとも一部のデータと、文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成し、文書データＭのみに依存する整数ｍと、点Ｒに依存する整数ｒと、署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、システム情報と、署名者の公開鍵Ｙが与えられたときに、±ｓ・Ｇ＝±ｍ・Ｙ±ｒ・Ｒ over Ｅ／Ｆｑで定義される関係式を用いて署名検査を行なう工程を具備する。



1

【特許請求の範囲】

【請求項１】　文書データＭに対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、

有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを用いて、

任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成する署名データ生成工程と、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、

$\pm s \cdot G = \pm m \cdot Y \pm r \cdot R$ over Ｅ／Ｆｑ

（＋、－の符号は所定の条件により決定）で定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項２】　文書データＭに対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、

有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを用いて、

任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成する署名データ生成工程と、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと前記公開鍵Ｙとの積からなる第２の項ｍ・Ｙと、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

2

【請求項３】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、

第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i = x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、

複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと複数の署名者の各々に対する秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成する署名データ生成工程と、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、

$\pm s \cdot G = \pm m \cdot (Y_1 + Y_2 + \cdots + Y_n) \pm r \cdot R$ over Ｅ／Ｆｑ

（＋、－の符号は所定の条件により決定）で定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項４】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成し、この電子署名データに基づいて複数の署名者の署名検査を行なう電子署名方法であって、

第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i = x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、

複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと複数の署名者の各々に対する秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成する署名データ生成工程と、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、

前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと各公開鍵Y_i

3

（ｉ＝１，２，３，…，ｎ）の和との積からなる第２の項ｍ・（Y_1 ＋Y_2 ＋…＋Y_n）と、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項５】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成し、この電子署名データに基づいて複数の署名者の署名検査を行なう電子署名方法であって、

第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i = x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、

複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の各点R_iの少なくとも一部のデータと、前記文書データＭと複数の署名者の各々に対する秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成する署名データ生成工程と、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の各点Ｒｉ及び前記文書データＭのうち少なくとも点R_iに依存する各整数r_iと、前記署名データである各点R_iの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、

前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと各公開鍵Y_i（ｉ＝１，２，３，…，ｎ）の和との積からなる第２の項ｍ・（Y_1 ＋Y_2 ＋…＋Y_n）と、前記整数r_iと前記楕円曲線Ｅ／Ｆｑ上の各点R_iとの積の和からなる第３の項（$r_1 R_1 + r_2 R_2 + \cdots + r_n R_n$）との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項６】　文書データＭに対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて署名検査を行なう署名検査装置とから構成される電子署名システムであって、

前記署名データ作成装置は、

有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを用いて、

任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基

4

点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成する手段を含み、

前記署名検査装置は、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと前記公開鍵Ｙとの積からなる第２の項ｍ・Ｙと、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含むことを特徴とする電子署名システム。

【請求項７】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて複数の署名者の署名検査を行なう署名検査装置とから構成される電子署名システムであって、

前記署名データ作成装置は、

第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i = x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、

複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成する手段を含み、

前記署名検査装置は、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、

前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと各公開鍵Y_i（ｉ＝１，２，３，…，ｎ）の和との積からなる第２の項ｍ・（Y_1 ＋Y_2 ＋…＋Y_n）と、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含むことを特徴とする電子署名シス

5

テム。

【請求項８】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて複数の署名者の署名検査を行なう署名検査装置とから構成される電子署名システムであって、

前記署名データ作成装置は、

第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i = x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、

複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の各点R_iの少なくとも一部のデータと、前記文書データＭと複数の署名者の各々に対する秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成する手段を含み、

前記署名検査装置は、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の各点R_i及び前記文書データＭのうち少なくとも点R_iに依存する各整数r_iと、前記署名データである各点R_iの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、

前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと各公開鍵Y_i（ｉ＝１，２，３，…，ｎ）の和との積からなる第２の項$m \cdot (Y_1 + Y_2 + \cdots + Y_n)$と、前記整数$r_i$と前記楕円曲線Ｅ／Ｆｑ上の各点$R_i$との積の和からなる第３の項$(r_1 R_1 + r_2 R_2 + \cdots + r_n R_n)$との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含むことを特徴とする電子署名システム。

【請求項９】　文書データＭに対する電子署名データを作成する処理と、作成された電子署名データに基づいて署名検査を行なう処理とをコンピュータに実行させる命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、

前記電子署名データを作成する処理は、

有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵$Y = x \cdot G$を満たすように作成された署名者の秘密鍵ｘとを用いて、

任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成し、

6

前記署名検査を行なう処理は、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、

前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと前記公開鍵Ｙとの積からなる第２の項ｍ・Ｙと、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう、ことを特徴とする記録媒体。

【請求項１０】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成する処理と、作成された電子署名データに基づいて複数の署名者の署名検査を行なう処理とをコンピュータに実行させる命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、

前記電子署名データを作成する処理は、

第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i = x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、

複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと複数の署名者の各々に対する秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成し、

前記署名検査を行なう処理は、

前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、

前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと各公開鍵Y_i（ｉ＝１，２，３，…，ｎ）の和との積からなる第２の項$m \cdot (Y_1 + Y_2 + \cdots + Y_n)$と、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう、ことを特徴とする記録媒体。

【請求項１１】　ｎ者から構成される複数の署名者の間で文書データＭに対する電子署名データを作成する処理と、作成された電子署名データに基づいて複数の署名者の署名検査を行なう処理とをコンピュータに実行させる

命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、
前記電子署名データを作成する処理は、
第ｉ番目（ｉ＝１，２，３，…，ｎ）の署名者について、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Y_iと、この公開鍵$Y_i=x_i \cdot G$を満たすように作成された署名者の秘密鍵x_iとを用いて、
複数の署名者の各々に対して生成された各乱数k_iと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の各点R_iの少なくとも一部のデータと、前記文書データＭと複数の署名者の各々に対する秘密鍵x_iと各乱数k_iとに依存する整数ｓとを含む署名データを生成し、
前記署名検査を行なう処理は、
前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の各点R_i及び前記文書データＭのうち少なくとも点R_iに依存する各整数r_iと、前記署名データである各点R_iの少なくとも一部のデータ及び整数ｓと、前記システム情報と、各公開鍵Y_iが与えられたときに、
前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと各公開鍵Y_i（ｉ＝１，２，３，…，ｎ）の和との積からなる第２の項$m \cdot (Y_1 + Y_2 + \cdots + Y_n)$と、前記整数$r_i$と前記楕円曲線Ｅ／Ｆｑ上の各点$R_i$との積の和からなる第３の項$(r_1 R_1 + r_2 R_2 + \cdots + r_n R_n)$との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう、ことを特徴とする記録媒体。

＊【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子的な文書に対する署名、捺印機能を実現する電子署名方法及び、この電子署名方法を用いて構成した電子署名システム、さらに、前記電子署名方法に関するプログラムが格納された記録媒体に関する。
【０００２】
【従来の技術】電子署名（ディジタル署名）の作成法として様々な方式が考案されている。この中で代表的なものは素因数分解問題の困難性に基づく方式と離散対数問題の困難性に基づく方式である。このうち離散対数問題に基づく方式は、一般的な有限体上の乗法群を利用する方式と楕円曲線上の加法群を利用する方式が存在する。楕円曲線上の加法群における離散対数問題は有限体上の乗法群における離散対数問題や素因数分解問題に比べ、効率的な解法が発見されておらず、より安全性が高いといわれている。
【０００３】従って、同じ安全性を確保してディジタル署名や公開鍵暗号方式を構成する場合、楕円曲線上の離散対数問題をベースに構築したシステムは他の問題をベースにした場合と比べてパラメータのサイズを小さく設定することが可能であり、このことが処理量の削減にもつながるという効果があることが知られている。
【０００４】有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑは、有限体Ｆｑの標数が２もしくは３以外の場合、次式（１）中のパラメータａ，ｂと有限体Ｆｑで定義される。楕円曲線Ｅ／Ｆｑは標数が２もしくは３の場合にも定義可能であるがここでは省略する。
【０００５】

$$y^2 = x^3 + ax + b \quad (1)$$

（但しａ，ｂ，ｘ，ｙは有限体Ｆｑの元）

ここで、ｙ＾２はｙの２乗を表し、ｘ＾３はｘの３乗を表すものとする。以下、ｘ＾ａでｘのａ乗を表す。
【０００６】楕円曲線Ｅ／Ｆｑの元は式（１）を満たす（ｘ，ｙ）のペア（これを楕円曲線上の点と呼ぶ）と、無限遠点Ｏとから成る。無限遠点Ｏは有限体Ｆｑの元のペア（ｘ，ｙ）という形式では表現できないが、実装上は無限遠点を表す１ビットのフラグを用意すれば良い。この楕円曲線上の点の集合は加算に関して群を構成することが知られている。この加算に関して無限遠点Ｏは単位元になる。
【０００７】楕円曲線Ｅ／Ｆｑのより詳細な説明や加算の定義などは例えばKoblitz, “A Course in Number Theory and Cryptography”, Springer-Verlag にある。以下では特に断らない限り大文字で楕円曲線上の点（すなわち、有限体Ｆｑの元のペアもしくは無限遠点）を表し、小文字では有限体Ｆｑの元もしくは自然数を表すこととする。なお、有限体Ｆｑはｑ＝ｐ＾ｔ（但しｐは素数、ｔは正整数）個の元から成り、例えば、素体Ｚｐ（０からｐ－１までの整数で構成される）や２の拡大体ＧＦ（２＾ｔ）が典型的である。
【０００８】楕円曲線上のディジタル署名方式の代表的な方式に楕円曲線上のElGamal 署名がある。この方式では、公開鍵として楕円曲線を定義する有限体Ｆｑ，ａ，ｂ、基点Ｇ、基点Ｇの位数ｚを用いる。但し、基点Ｇの位数ｚとは、$z \cdot G = O$ over Ｅ／Ｆｑを満たす最小の正整数を表す。
【０００９】署名作成者の秘密鍵は位数ｚと互いに素でｚ未満の整数ｘであり、署名作成者の公開鍵は以下の点Ｙである。

$$Y = x \cdot G \text{ over } E/Fq$$

文書データＭのみに依存する整数ｍ（これは一般にディジタルビット列で表現した文書データＭを暗号的なハッシュ関数により計算したダイジェスト情報である）に対するディジタル署名は以下の手順により作成される。ま

ず、位数ｚと互いに素でｚ未満の自然数である乱数ｋを決定し、このｋから次式のＲを求める。

【００１０】Ｒ＝ｋ・Ｇ over Ｅ／Ｆｑ

次に、楕円曲線上の点データをＺｚ（ｚ－１以下の自然数）の中へ変換する関数ｆを用いて、以下のｒを求める。例えば、ハッシュ関数を用いれば良い。

【００１１】ｒ＝ｆ（Ｒ）

さらに、以下のｓを求める。

ｓ＝（ｍ－ｘ・ｒ）／ｋ（mod ｚ）

署名データは（Ｒ，ｓ）のペアである。署名の検査は、ｍ，Ｒ，ｓが次式を満たすことを検査することによって行われる。

【００１２】ｒ＝ｆ（Ｒ）

ｍ・Ｇ＝ｒ・Ｙ＋ｓ・Ｒ over Ｅ／Ｆｑ

ElGamal 署名方式(ElGamal signature scheme)は、“T.ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. IT, Vol.IT-31, No.4, July 1985, pp.469-472”に詳細に記載されている。

【００１３】以上の電子署名方式により一般の電子文書に対する捺印機能を実現することができるが、さらに、電子的な回覧文書に対する複数の署名者(signer)による捺印機能も要望される。このような機能は複数の署名者による同一の文書に対する署名データを連結することで構成できる。しかし、このような構成では署名者数に比例して署名データ量と署名検査の処理量が増加する欠点がある。単純に個別の署名を連結する場合に比べて、署名データサイズの増加が少なく抑えられる方式、あるいは、署名検査の処理量が抑えられる方式が考案されており、これらは多重署名法と呼ばれている。

【００１４】

【発明が解決しようとする課題】しかしながら、上記した多重署名法は、楕円曲線上の離散対数問題の困難性に基づくElGamal 署名方式を用いたものではなかった。本発明はこのような課題に着目してなされたものであり、その目的とするところは、様々な運用形態を考慮した多重署名システムを容易に構成できる楕円曲線を利用した電子署名方法、及びこの電子署名方法を用いて構成した電子署名システム、さらには前記電子署名方法に関するプログラムが格納された記録媒体を提供することにある。

【００１５】

【課題を解決するための手段】上記の目的を達成するために、本発明の電子署名方法は、文書データＭに対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを

用いて、任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成する署名データ生成工程と、前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、±ｓ・Ｇ＝±ｍ・Ｙ±ｒ・Ｒ over Ｅ／Ｆｑ（＋、－の符号は所定の条件により決定）で定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程とを具備する。

【００１６】また、本発明の電子署名システムは、文書データＭに対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて署名検査を行なう署名検査装置とから構成される電子署名システムであって、前記署名データ作成装置は、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを用いて、任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成する手段を含み、前記署名検査装置は、前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと前記公開鍵Ｙとの積からなる第２の項ｍ・Ｙと、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含む。

【００１７】また、本発明の記録媒体は、文書データＭに対する電子署名データを作成する処理と、作成された電子署名データに基づいて署名検査を行なう処理とをコンピュータに実行させる命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、前記電子署名データを作成する処理は、有限体Ｆｑ上の楕円曲線Ｅ／Ｆｑと、この楕円曲線Ｅ／Ｆｑ上の基点Ｇとを含むシステム情報と、前記楕円曲線Ｅ／Ｆｑ上の点で定義される署名者の公開鍵Ｙと、この公開鍵Ｙ＝ｘ・Ｇを満たすように作成された署名者の秘密鍵ｘとを用い

て、任意に生成された乱数ｋと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとに依存する楕円曲線Ｅ／Ｆｑ上の点Ｒの少なくとも一部のデータと、前記文書データＭと秘密鍵ｘと乱数ｋとに依存する整数ｓとを含む署名データを生成し、前記署名検査を行なう処理は、前記文書データＭのみに依存する整数ｍと、前記楕円曲線Ｅ／Ｆｑ上の点Ｒ及び前記文書データＭのうち少なくとも点Ｒに依存する整数ｒと、前記署名データである点Ｒの少なくとも一部のデータ及び整数ｓと、前記システム情報と、前記署名者の公開鍵Ｙが与えられたときに、前記整数ｓと前記楕円曲線Ｅ／Ｆｑ上の基点Ｇとの積からなる第１の項ｓ・Ｇと、前記整数ｍと前記公開鍵Ｙとの積からなる第２の項ｍ・Ｙと、前記整数ｒと前記楕円曲線Ｅ／Ｆｑ上の点Ｒとの積からなる第３の項ｒ・Ｒとの間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう。

【００１８】

【発明の実施の形態】まず、本実施形態の概略を説明する。第１の概略に係る電子署名方式は、楕円曲線上のElGamal 署名方式を変形した電子署名方式であり、従来の楕円曲線上のElGamal 署名方式との相違点は、署名検査式における文書データＭと、署名データｓと、乱数から生成された署名データＲ及び文書データＭのうち少なくとも署名データＲに依存する整数ｒの各々を互いに所定の規則に基づいて置き換えたことにある。各署名者の秘密鍵が作用したｓがｓ＝ｍ・ｘ＋ｒ・ｋ（mod ｚ）という形式で作成されるので、秘密鍵ｘが複数になっても、多重署名の場合は文書データＭが共通なので、複数の秘密鍵ｘが加算によりまとめられる。このことにより、同方式の多重署名方式への拡張が容易になるという利点が得られる。

【００１９】なお、ｒ・ｋは秘密鍵ｘが複数になっても影響を受けない項であるから、整数ｒは乱数から生成された点Ｒのみに依存させる構成以外に、点Ｒと文書データＭの両方に依存させる構成でもよく、その方が安全性の向上が期待できる。

【００２０】このように楕円曲線上のElGamal 署名方式を変形しても公開鍵Ｙに対応する秘密鍵ｘを保持する署名者は検査式を満たす署名データＲ，ｓを作成できる。一方、秘密鍵ｘを保持しない場合に署名データＲ，ｓを求めるには、楕円曲線上の離散対数問題を求める以外の方法は考案されていない。従って、電子署名方式として有効である。

【００２１】次に第２の概略を説明する。第２の概略では、第１の概略における電子署名方式を多重署名方式として適用する。複数の署名者がそれぞれ乱数ｋを作成し、各々の乱数ｋに依存した楕円曲線上の点Ｒを最初にデータを一巡させることで作成する。その後、各々の署名者が自身の作成した乱数ｋと秘密鍵ｘから部分署名ｓを作成し、これを巡回する。

【００２２】部分署名ｓの巡回においては、それ以前の署名者による部分署名に各自の部分署名を融合させる。こうして最後の署名者の処理により多重署名データＲ，ｓが作成される。

【００２３】署名検査における検査式は第１の概略における検査式の公開鍵Ｙを複数の署名作成者の個々の公開鍵Ｙｉの和に置き換えたものである。秘密鍵ｘｉが一つでも関与しない場合には、検査式を満たすＲ，ｓは得られない。従って、複数の署名者による電子署名方式として有効である。

【００２４】次に第３の概略を説明する。第３の概略では、第１の概略における電子署名方式を逐次型（一巡型）の多重署名方式に適用する。複数の署名者がそれぞれ乱数ｋを作成し、この乱数ｋに依存した楕円曲線上の点Ｒを作成する。各署名者は、前の署名者から得た部分署名ｓに自分の秘密鍵ｘと点Ｒの生成に利用した乱数ｋを融合させて、新たな部分署名ｓを作成し、これを次の署名者に送る。この部分署名ｓと同時に、独立に生成した点を署名データの一部として追加していく。こうして最後の署名者の処理により多重署名データｓ，R_1，R_2，…，R_nが作成される。

【００２５】署名検査における検査式は第１の概略における検査式の公開鍵Ｙを複数の署名作成者の個々の公開鍵Y_iの和に置き換え、さらに点Ｒの項を個々の署名者による$r_i \cdot R_i$の和に置き換えたものを用いる。

【００２６】以下に、図面を参照して上記した概略を詳細に説明する。図１は本発明の第１実施形態に係る電子署名システムの基本構成を示す図である。図１に示すように、本システムはセンタ１０と利用者に対応する複数の局(entities)１１、１２、１３（U_1、U_2、…、U_i）から成る通信ネットワーク１４により構成される。センタ１０は公開情報として、楕円曲線Ｅ／Ｆｑのパラメータを生成して公開する。また、楕円曲線Ｅ／Ｆｑ上の基点Ｇとその位数ｚを求めて公開する。

【００２７】さらに、関数ｆと関数ｈを公開する。これらは暗号的なハッシュ関数であり、任意のサイズの入力に対し、そのダイジェスト情報として１６０bit 程度の固定長の整数を出力する。具体例は、ＳＨＡやＭＤ５、ＲＩＰＥ－ＭＤなどである。また、関数ｆとｈは共通でも良い。

【００２８】各局U_iはｚ－１以下の自然数である乱数x_iを定め、このx_iを局秘密鍵とする。さらに、局公開鍵Y_iを次式により定める。

$Y_i = x_i \cdot G$ over Ｅ／Ｆｑ

局U_iは局公開鍵Y_iをセンタ１０に送り、センタ１０は公開鍵リストの局U_iのエリアにY_iを登録する。公開鍵リストの書き換えはセンタ１０のみが実行でき、同リストの読み出しは任意の局が実行できる。なお、局U_iのＩＤ情報（識別情報）をI_iとする。

【００２９】図２Ａは、局U_iが文書データＭに対する

ディジタル署名を作成する手順である。

＜局U_iの手順＞

１：乱数ｋ（１＜ｋ＜ｚ－１）を定める。…（ステップ１０１）

２：Ｒ＝ｋ・Ｇ over Ｅ／Ｆｑを計算する。…（ステップ１０２）

３：ｒ＝ｆ（Ｒ）を計算する。…（ステップ１０３）

４：ｍ＝ｈ（Ｍ）を計算する。…（ステップ１０４）

５：ｍ，ｒと秘密鍵x_iからｓ＝x_i・ｍ＋ｋ・ｒ mod ｚを計算する。

【００３０】…（ステップ１０５）

以上により作成されたＲとｓが局U_iの文書データＭに対するディジタル署名となる。

【００３１】この署名作成手続きにおけるステップ１０１から１０３は、文書データＭに依存しないため、ディジタル署名作成の要求が生じる前に計算し、（ｋ，Ｒ，ｒ）を幾つか蓄積しておくことができる。このようにすると、署名作成要求時の処理はステップ１０４，１０５のみとなり、処理時間面で有効である。

【００３２】次に図２Ｂを参照しながら、本ディジタル署名の検査手順を説明する。

＜署名検査手順＞

１：公開リストから局U_iの公開鍵Y_iを取り出す。

【００３３】…（ステップ１０６）

２：ｒ＝ｆ（Ｒ）を計算する。…（ステップ１０７）

３：ｍ＝ｈ（Ｍ）を計算する。…（ステップ１０８）

４：ｒ．ｓ，ｍ，Y_iが次式の関係を満たすことを確認＊

$$(s/r)\cdot G-(m/r)\cdot Y_i = R \text{ over } E/Fq,$$
$$(s/m)\cdot G-(r/m)\cdot R = Y_i \text{ over } E/Fq,$$
$$(m/s)\cdot Y_i+(r/s)\cdot R = G \text{ over } E/Fq$$

などを検査することと等価であることは、検査式における左辺もしくは右辺の項の移項とｓ，ｍ，ｒのＦｑにおける逆数を両辺に掛けることから明らかである。

【００３８】また、検査式におけるｓ・Ｇ，ｍ・Y_i，ｒ・Ｒの３項の符号を変えること（すなわち、＋を－にしたり、その逆、具体的には±ｓ・Ｇ＝±ｍ・Y_i ±ｒ・Ｒ＝Ｏ over Ｅ／Ｆｑでもよく、＋、－の符号は以下の説明の通り、署名生成過程におけるステップにより決定される）も署名生成課程におけるステップ１０５のｓ，x_i・ｍ，ｋ・ｒの符号を変えることに相当するため、検査式における３項の符号を変えた署名方式は本質的に本実施形態の方式と同値であることにも注意されたい。

【００３９】なお、本発明の署名方式において、ｆ（Ｒ）の代わりにｆ（Ｒ，Ｍ）を用いてもよい。ｆ（Ｒ，Ｍ）は署名者がランダムに決定した、楕円曲線上の点Ｒのデータと文書データＭの両方に依存したハッシュ値を表している。具体的にはＲとＭとを連結してハッシュする、Ｒのデータを鍵として鍵付きハッシュ（Keyed hash）法を利用するなどである。

＊する。

【００３４】…（ステップ１０９）

ｓ・Ｇ＝ｍ・Y_i＋ｒ・Ｒ over Ｅ／Ｆｑ

この関係が成立する場合には、（Ｒ，ｓ）は局U_iの文書データＭに対するディジタル署名であるものと判定する。

【００３５】ステップ１０１から１０５の手順により生成された（Ｒ，ｓ）がステップ１０９の検査式を満足することは明らかである。逆に文書データＭが与えられた状態で、Y_iの離散対数x_iを持たない局がステップ１０９の検査式を満たす（Ｒ，ｓ）の組を求めることは楕円曲線上の離散対数問題を求めることと同程度に困難であると考えられる。例えば、最初にＲを定めるとｓ・Ｇ＝ const over Ｅ／Ｆｑなるｓを求めることになり、これは離散対数問題に他ならない。一方、ｓを先に定めるとｒ・Ｒ＝ const over Ｅ／Ｆｑなるを求めることになり、この解法も一般に知られていない。

【００３６】なお、本実施形態のディジタル署名方法で用いられる署名検査式の変形には様々なものが考えられるが、以下に代表的なものを示す。これらは本質的に同じ検査を実行していることに注意されたい。

【００３７】まず、ステップ１０９の検査式は、

ｓ・Ｇ－ｍ・Y_i－ｒ・Ｒ＝Ｏ over Ｅ／Ｆｑ，

－ｓ・Ｇ＋ｍ・Y_i＋ｒ・Ｒ＝Ｏ over Ｅ／Ｆｑ

などを検査することと等価であることは検査式における左辺もしくは右辺の項を移項することから明らかである。さらに、

$$(s/r)\cdot G-(m/r)\cdot Y_i = R \text{ over } E/Fq, \quad \cdots(2)$$

などを検査することと等価であることは、検査式における左辺もしくは右辺の項の移項とｓ，ｍ，ｒのＦｑにおける逆数を両辺に掛けることから明らかである。

【００４０】変形手順ではステップ１０３とステップ１０７がｒ＝ｆ（Ｒ，Ｍ）に変更される。一般にはこのように変形した手順の方が、ＲとＭからｒが作成されたことが保証されるために安全性が向上する。

【００４１】本実施形態の特徴は、署名者が署名作成毎に生成する乱数と基点Ｇに依存した項ｒ・Ｒと署名者の公開鍵Y_iと署名対象である文書データＭのみに依存した項ｍ・Y_iと署名者の秘密鍵x_iが作用したｓにより基点Ｇを加算する回数を変化させた項ｓ・Ｇの３つの項の加算が無限遠点に一致するかどうかを判定することにある。

【００４２】このうち式（２）を検査式とする場合には、署名データサイズの削減が可能である。以下にその具体的な手順を示す。局U_iが文書データＭに対するディジタル署名を作成する手順は基本的に先の手順と同じであるが、ステップ１０７におけるｒが位数ｚと互いに素であるかどうかを確認する。もし、互いに素でない場合には、ステップ１０１に戻り別の乱数ｋを生成する。最終的に出力されるディジタル署名のデータはｒとｓであり点Ｒの代わりにｒを用いる。このことにより署名デ

15

ータサイズが約２／３にできる。

【００４３】次に上記した検査手順を変形したディジタル署名の検査手順を図３を参照して説明する。

＜署名検査手順＞

１：公開リストから局U_iの公開鍵Y_iを取り出す。

【００４４】…（ステップ１１０１）

２：m＝h（M）を計算する。…（ステップ１１０２）

３：１／r（ｍｏｄＺ）を計算する。…（ステップ１１０３）

４：次式の点Rを計算する。…（ステップ１１０４）

$R=(s/r)\cdot G-(m/r)\cdot Y_i$ over E／Fq

５：点Rと署名データのrが次式の関係を満たすことを確認する。

【００４５】…（ステップ１１０５）

$r=f(R)$

この関係が成立する場合には、（r，s）は局U_iの文書データMに対するディジタル署名であるものと判定する。

【００４６】次に、図１に示したディジタル署名を多重署名に適用した第２実施形態の電子署名方法を説明する。図４Ａ、４Ｂは多重署名における情報の流れを表し、図５Ａ、５Ｂは各局の処理手順を表す。

【００４７】ここでは、局U_1，U_2，…U_nのｎ局が文書データMに多重署名する場合を想定する。多重署名の作成は図４ＡのR_nの作成ラウンドと、図４Ｂのs_nの作成ラウンドの２回の巡回操作から成る。図５ＡはR_nの作成ラウンドにおける局U_iの処理手順、図５Ｂはs_nの作成ラウンドにおける局U_iの処理手順をそれぞれ示す。

（１）R_nの作成ラウンド

＜局U_iの手順＞（ｉ＝１，２，…，ｎ）

１：乱数k_i（$1<k_i<z-1$）を作成する。…（ステップ３０１）

２：局$U_{(i-1)}$から受信した情報$R_{(i-1)}$と乱数k_iから次式のR_iを作成する。

【００４８】$R_i=R_{(i-1)}+k_i\cdot G$ over E／Fq …（ステップ３０２）

３：情報R_i，文書データMを局$U_{(i+1)}$に送信する。…（ステップ３０３）

以上の処理を局U_1から順番に局U_nまで実行し、R_nを作成する。なお、局U_1は、R_0＝O（無限遠点）としてステップ３０２の処理を行う。

【００４９】また、局U_nは作成した情報R_nからr＝f（R_n）によりrを求め、これを局U_1に送信し、s_nの作成ラウンドに移る。

（２）s_nの作成ラウンド

＜局U_iの手順＞（ｉ＝１，２，…，ｎ）

１：局U_1，U_2，…，$U_{(i-1)}$の公開鍵Y_1，Y_2，…，$Y_{(i-1)}$を公開鍵リストから取り出す。…（ステップ３０４）

16

２：局$U_{(i-1)}$からR_nの作成ラウンドで受信した$R_{(i-1)}$と、このラウンドで局$U_{(i-1)}$から受信したr，$s_{(i-1)}$が次の関係を満たしていることを確認する。…（ステップ３０５）

m＝h（M）を計算、

$s_{i-1}\cdot G=m\cdot(Y_1+Y_2+\cdots+Y_{i-1})+r\cdot R_{i-1}$ over E／Fq

３：ステップ３０５の関係を満足していない場合には、局U_{i-1}の処理に異常があったものとして処理を打ち切る。…（ステップ３０６）

４：先のラウンドで作成した乱数k_iと自局の秘密鍵x_iを用いて次式のs_iを計算する。…（ステップ３０７）

$s_i=s_{i-1}+x_i\cdot m+k_i\cdot r \mod z$

５：s_i，rを局U_{i+1}に送る。…（ステップ３０８）

以上の処理を局U1から順番に局U_nまで実行し、s_nを作成する。なお、局U_1は、s_0＝０としてステップ３０７の処理を行う。

【００５０】以上により作成された（R_n，s_n）が局U_1からU_nによる文書データMに対する多重署名である。局U_nは作成した署名情報（R_n，s_n）を必要に応じて全ての局U_1，U_2，…，U_{n-1}に送る。

【００５１】なお、上記手順のうちステップ３０４，３０５，３０６は部分署名s_{i-1}の検査を実行する部分であり、省略することも可能である。この部分署名の検査を省略した場合、多重署名（R_n，s_n）が作成された後になってはじめて検査を実行することになる。署名作成者の不正をできるだけ早期に検出するためにはステップ３０４，３０５，３０６の部分署名の検査が有効である。

【００５２】図６は図５Ａ，５Ｂの手順により作成された多重署名の検査手順を示す。検査時には以下の処理を行う。署名検査にはR_n，s_n，Mおよび局のＩＤ情報I_1，I_2，…，I_nが必要である。

【００５３】１：局U_1，U_2，…，U_nの公開鍵Y_1，Y_2，…，Y_nを公開鍵リストから取り出す。…（ステップ４０１）

２：R_n，s_n，Mが次の関係を満たすことを確認する。…（ステップ４０２）

m＝h（M）を計算、

r＝f（R_n）を計算、

$s_n\cdot G=m\cdot(Y_1+Y_2+\cdots+Y_n)+r\cdot R_n$ over E／Fq

この関係が成立する場合には、（R_n，s_n）は正当な多重署名であるものと判定する。

【００５４】なお、以上に示した多重署名作成手順及び多重署名検査手順でもr＝f（R_n）の代わりにr＝f（R_n、M）に変更し、さらに多重署名検査手順におけるステップ４０２においてr＝f（R_n、M）に変更することもできる。

17

【００５５】次に、図３に示した署名検査手順をこの多重署名に適用する手順を説明する。局U_iが文書データMに対するディジタル署名を作成する手順は基本的に図５Ａ，５Ｂの手順と同じであるが、ここでは、局U_nにおけるステップ３０２における計算の結果として生じるR_nに対しｒ＝ｆ（R_n）を計算し、ｒが位数ｚと互いに素かどうかを確認する。もし、互いに素でない場合には、ステップ３０１に戻り別の乱数k_nを生成する。R_nの生成ラウンドで局U_nが出力するｒはｚと互いに素である。また、２巡目が終了して最終的に出力される多重署名のデータはｒとs_nである。

【００５６】次にこのディジタル署名の検査手順を説明する。図７はこの手順により作成された多重署名の検査手順を示す。

１：局U_1，U_2，U_nの公開鍵Y_1，Y_2，…，Y_nを公開鍵リストから取り出す。…（ステップ１２０１）

２：ｍ＝ｈ（Ｍ）を計算…（ステップ１２０２）

３：１／ｒ（ｍｏｄ　Ｚ）を計算する。…（ステップ１２０３）

４：次式の点R_nを計算する。…（ステップ１２０４）

$R_n = (s_n / r) \cdot G - (m / r) \cdot (Y_1 + Y_2 + \cdots + Y_n)$ over E／F q

５：点R_nと署名データのｒが次式の関係を満たすことを確認する。…（ステップ１２０５）

$r = f(R_n)$

この関係が成立する場合には、（ｒ，s_n）は正当な多重署名であるものと判定する。

【００５７】次に、図２Ａ、２Ｂに示したディジタル署名を多重署名に適用した第３実施形態の電子署名方法を説明する。第３実施形態における情報の流れを図８に示す。ここでは複数の署名作成局間で情報を１巡させるだけで多重署名データを生成する。局U_1，U_2，…，U_nのｎ局が多重署名を作成するものとする。図９は局U_iの手順を示す。

＜局U_iの手順＞（ｉ＝１，２，…，ｎ）

１：局U_1，U_2，…，U_{i-1}の公開鍵Y_1，Y_2，…，Y_{i-1}を公開鍵リストから取り出す。…（ステップ６０１）

２：局U_{i-1}から受信したR_1，R_2，…，R_{i-1}，s_{i-1}，Ｍが次の関係を満たしていることを確認する。…（ステップ６０２）

ｍ＝ｈ（Ｍ）を計算、

$r_j = f(R_j)$（ｊ＝１，２，…，ｉ－１）を計算、

$s_{i-1} \cdot G = m \cdot (Y_1 + \cdots + Y_{i-1}) + r_1 \cdot R_1 + r_2 \cdot R_2 + \cdots r_{i-1} \cdot R_{i-1}$ over E／F q

３：ステップ６０２の関係を満足していない場合には、局U_{i-1}の処理に異常があったものとして処理を打ち切る。…（ステップ６０３）

４：乱数k_i（$1 < k_i < z - 1$）を作成する。…（ステップ６０４）

18

５：乱数k_iから次式のR_iを作成する。…（ステップ６０５）

$R_i = k_i \cdot G$ over E／F q

６：局U_{i-1}から受信した情報s_{i-1}と乱数k_i，自局の秘密鍵x_iから次式のs_iを計算する。…（ステップ６０６）

$r_i = f(R_i)$を計算、

$s_i = s_{i-1} + x_i \cdot m + k_i \cdot r_i \bmod z$

７：データs_i，R_1，R_2，…，R_i，文書データMを局U_{i+1}に送信する。

【００５８】…（ステップ６０７）

以上の処理を局U_1から順番に局U_nまで実行し、作成されたs_n，R_1，R_2，…，R_nが局U_1からU_nによる文書データMに対する多重署名である。なお、局U_1は、R_o＝Ｏ（無限遠点），s_o＝０としてステップ６０５，６０６の処理を行い、ステップ６０１から６０３までの部分署名の検査処理は行わない。

【００５９】図９の手順により作成された多重署名の検査手順を図１０を参照しながら説明する。

１：局U_1，U_2，U_nの公開鍵Y_1，Y_2，…，Y_nを公開鍵リストから取り出す。…（ステップ７０１）

２：s_n，R_1，R_2，…，R_n，Ｍが次の関係を満たすことを確認する。

【００６０】…（ステップ７０２）

ｍ＝ｈ（Ｍ）を計算、

$r_j = f(R_j)$（ｊ＝１，２，…，ｉ－１）を計算、

$s_n \cdot G = m \cdot (Y_1 + \cdots + Y_n) + r_1 \cdot R_1 + r_2 \cdot R_2 + \cdots r_n \cdot R_n$ over E／F q

この関係が成立する場合には、（s_n，R_1，R_2，…，R_n）は正当な多重署名であるものと判定する。

【００６１】なお、図９，図１０に示した多重署名法は、図５Ａ、５Ｂ，図６の多重署名法に比べて、データ・サイズと検査時の処理量からは不利であるが、署名作成が１巡の処理で行えるという利点を持つ。

【００６２】また、他の実施形態と同様に本多重署名手順でもｒ＝ｆ（R_i）の代わりにｒ＝ｆ（R_i，Ｍ）を利用してもよい。具体的には、局U_iの多重署名作成手順におけるステップ６０２にて$r_j = f(R_j, M)$（ｊ＝１，２，…，ｉ－１）を計算し、ステップ６０６にて、$r_i = f(R_i, M)$を計算するようにそれぞれ変更する。

【００６３】多重署名の検査手順では、ステップ７０２にて$r_j = f(R_j, M)$（ｊ＝１，２，…，ｉ－１）を計算するように変更する。図１１は、本実施形態の電子署名方式の作成・検査を実行する装置の一構成を示す。

【００６４】演算器９０１は多倍長の演算を実行する部分であり、本電子署名方式の演算処理の大部分を実行する。乱数発生器９０２は署名作成時に必要な乱数ｋを生成する部分である。乱数メモリ９０３は乱数発生器９０

２で発生された乱数ｋと、乱数ｋから計算されるＲ＝ｋ・Ｇ over Ｅ／Ｆｑの値と、ｒ＝ｆ（Ｒ）の値のペアを蓄積する部分である。乱数発生器９０２，演算器９０１は署名作成時・検査時以外にも稼働し、乱数（ｋ，Ｒ，ｒ）のペアを生成し、乱数メモリ９０３に蓄積する。秘密鍵メモリ９０４は局の秘密鍵を格納するメモリである。その他に制御部９０５，メモリ９０６，入出力部９０７から構成される。

【００６５】最後に、本実施形態の署名方式の変形例を一つ示す。局U_iが文書データＭに対するディジタル署名を作成する手順は以下の通りである。

＜局U_iの手順＞

１：乱数ｋ（１＜ｋ＜ｚ－１）を定める。…（ステップ１００１）

２：Ｒ＝ｋ・Ｇ over Ｅ／Ｆｑを計算する。…（ステップ１００２）

３：ｒ＝ｆ（Ｒ）を計算する。…（ステップ１００３）

４：ｍ＝ｈ（Ｍ，Ｒ）を計算する。…（ステップ１００４）

５：ｍ，ｒと秘密鍵x_iからｓ＝x_i・ｍ＋ｋ・ｒ mod ｚを計算する。

【００６６】…（ステップ１００５）

以上により作成されたＲとｓが局U_iの文書データＭに対するディジタル署名となる。

【００６７】本ディジタル署名の検査手順は以下の通りである。

＜署名検査手順＞

１：公開鍵リストから局U_iの公開鍵Y_iを取り出す。

【００６８】

…（ステップ１００６）

２：ｒ＝ｆ（Ｒ）を計算する。…（ステップ１００７）

３：ｍ＝ｈ（Ｍ，Ｒ）を計算する。…（ステップ１００８）

４：ｒ，ｓ，ｍ，Y_iが次式の関係を満たすことを確認する。…（ステップ１００９）

ｓ・Ｇ＝ｍ・Y_i＋ｒ・Ｒ over Ｅ／Ｆｑ

この関係が成立する場合には、（Ｒ，ｓ）は局U_iの文書データＭに対するディジタル署名であるものと判定する。

【００６９】この方式ではｍの計算において、文書データＭのみでなくランダムに生成された点Ｒのデータを作用させてハッシングしている。一般にはこのようにした方が安全性が向上するものと考えられる。なお、ｍ＝ｈ（Ｍ，ｒ）としても良い。

【００７０】この変形方式における２巡型多重署名（図５Ａ、５Ｂおよび図６）の手順は単純にｍ＝ｈ（Ｍ，Ｒ）に置き換えれば良い。１巡型多重署名（図９および図１０）の手順では、署名者によりm_1＝ｈ（Ｍ，R_1），m_2＝ｈ（Ｍ，R_2），…，m_n＝ｈ（Ｍ，R_n）と異なるｍが生成されるので、検査式もs_i・Ｇ＝m_1・Y_1＋…＋m_n・Y_n＋r_1・R_1＋…＋r_n・R_nと変更される。

【００７１】また、図１２Ａ、１２Ｂに示すような手順の多重署名方法を用いた場合でも、図３，図７に示した検査手順を適用することができる。以上のように、本実施形態によれば、楕円曲線上のElGamal 署名を変形し、２巡型や１巡型の多重署名を容易に構成可能な電子署名方法が提供できる。

【００７２】なお、上記した各実施形態における、電子署名データを作成する処理及び作成された電子署名データに基づいて署名検査を行なう処理は、プログラムとしてコンピュータが読み取り可能な記録媒体に格納し、コンピュータに実行させることが可能である。

【００７３】

【発明の効果】以上述べたように本発明によれば、様々な運用形態を考慮した多重署名システムを容易に構成できる電子署名方法、電子署名システム、及び記録媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る電子署名システムの基本構成を示す図である。

【図２】（ａ）は、本発明の第１実施形態に係る電子署名方法において、署名作成手順を示す図であり、（ｂ）は検査手順を示す図である。

【図３】本発明の第１実施形態に係る電子署名方法を変形した署名検査手順を示す図である。

【図４】本発明の第２実施形態に係る２巡式の多重署名方法における情報の流れを示す図である。

【図５】２巡式の多重署名方式の署名作成手順を示す図である。

【図６】２巡式の多重署名方式の検査手順を示す図である。

【図７】２巡式の多重署名方式を変形した署名検査手順を示す図である。

【図８】本発明の第３実施形態に係る１巡式の多重署名方法における情報の流れを示す図である。

【図９】１巡式の多重署名方法における署名作成手順を示す図である。

【図１０】１巡式の多重署名方法の検査手順を示す図である。

【図１１】電子署名データの作成及び検査を行なう装置の構成例を示す図である。

【図１２】署名手順の変形例を示す図である。

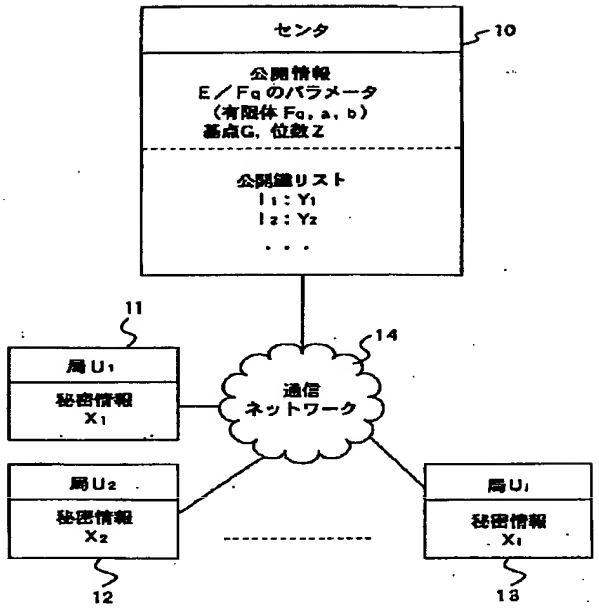
【符号の説明】

１０…センタ、

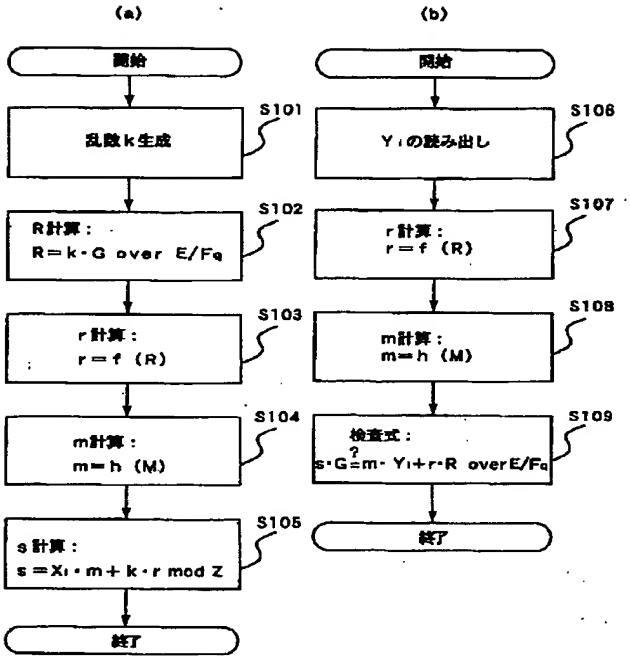
１１、１２、１３…局、

１４…通信ネットワーク。

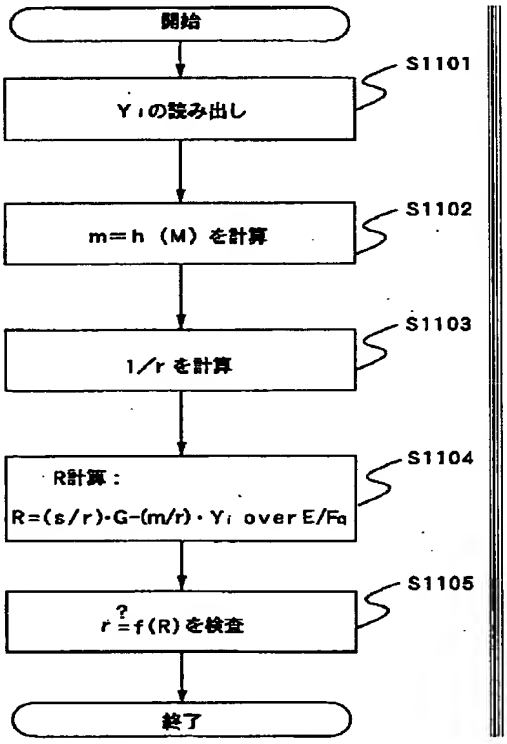
【図１】


センタ
10
公開情報
E／Fqのパラメータ
（有限体 Fq，a，b）
基点G，位数Z
公開鍵リスト
I1：Y1
I2：Y2
・・・
11
局U1
秘密情報
X1
14
通信
ネットワーク
局U2
秘密情報
X2
局Ui
秘密情報
Xi
12
13

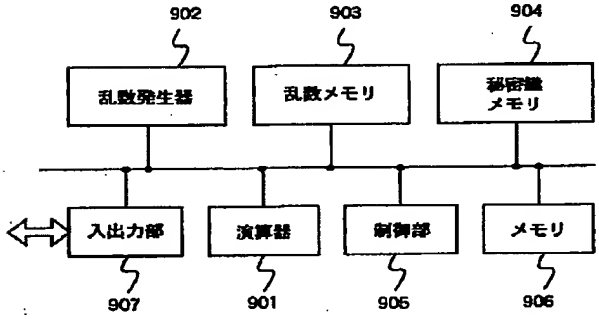
【図２】


(a)
(b)
開始
開始
乱数k生成
S101
Yiの読み出し
S106
R計算：
R＝k・G over E/Fq
S102
r計算：
r＝f（R）
S107
r計算：
r＝f（R）
S103
m計算：
m＝h（M）
S108
m計算：
m＝h（M）
S104
検査式：
s・G=?m・Yi+r・R overE/Fq
S109
s計算：
s＝Xi・m＋k・r mod Z
S105
終了
終了

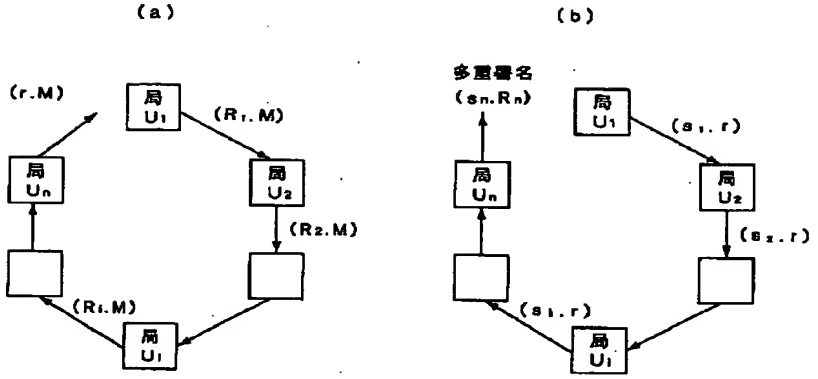
【図３】


開始
Yiの読み出し
S1101
m＝h（M）を計算
S1102
1/rを計算
S1103
R計算：
R=(s/r)-G-(m/r)・Yi overE/Fq
S1104
r=?f(R)を検査
S1105
終了

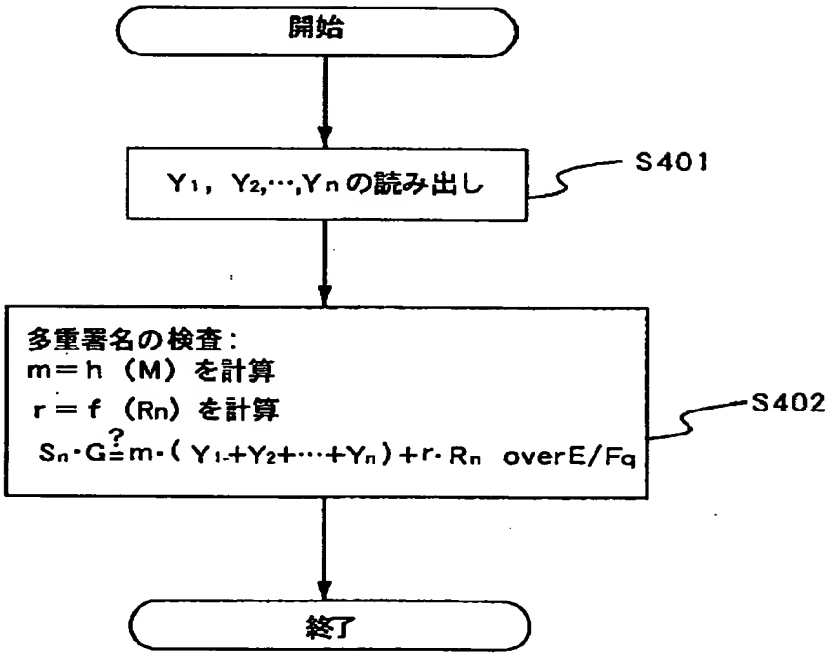
【図１１】


902
903
904
乱数発生器
乱数メモリ
秘密鍵
メモリ
入出力部
演算器
制御部
メモリ
907
901
905
906

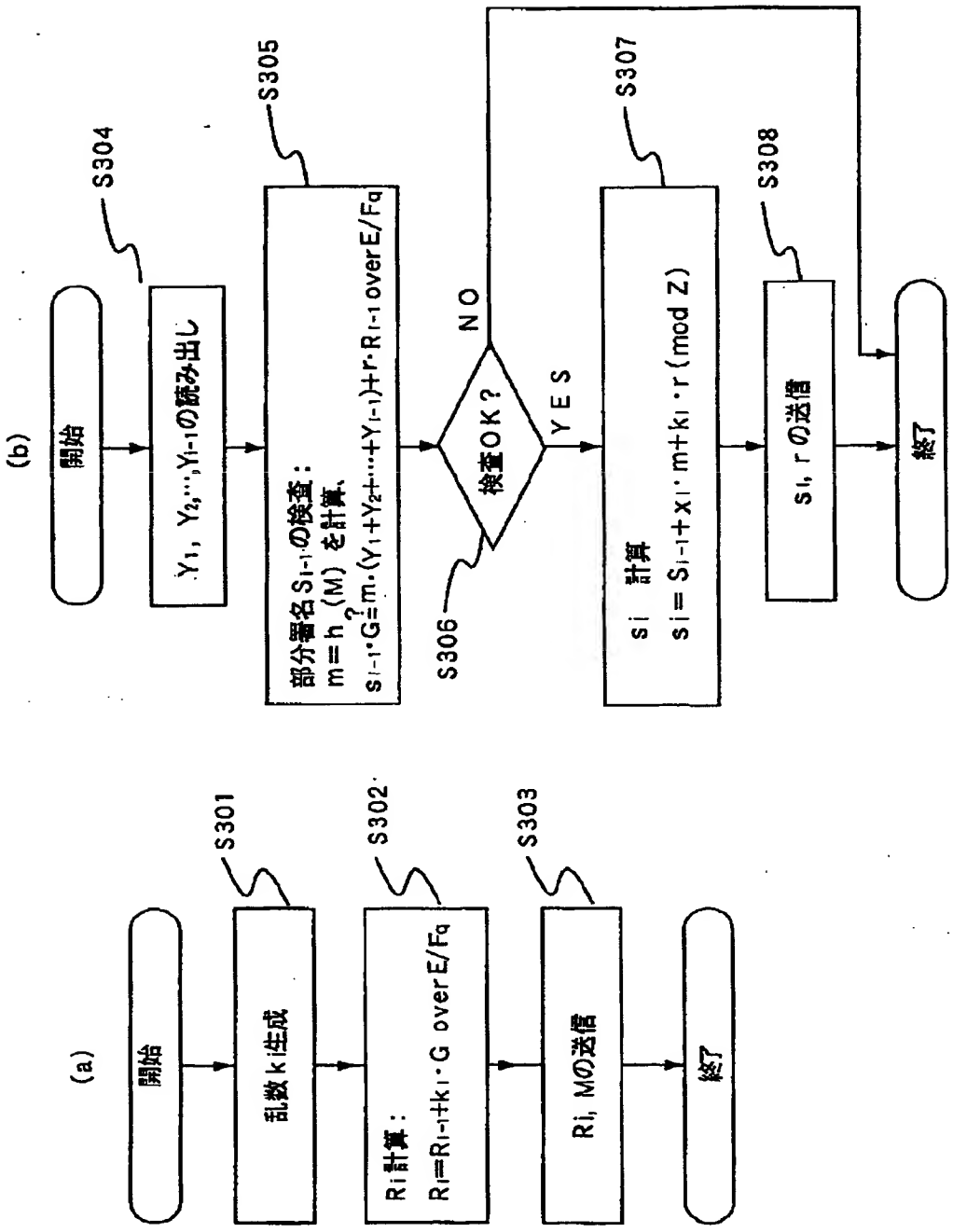
【図４】


(a)
(r.M)
局 U1
(R1.M)
局 Un
局 U2
(R2.M)
(Ri.M)
局 Ui
(b)
多重署名
(sn.Rn)
局 U1
(s1.r)
局 Un
局 U2
(s2.r)
(s1.r)
局 Ui

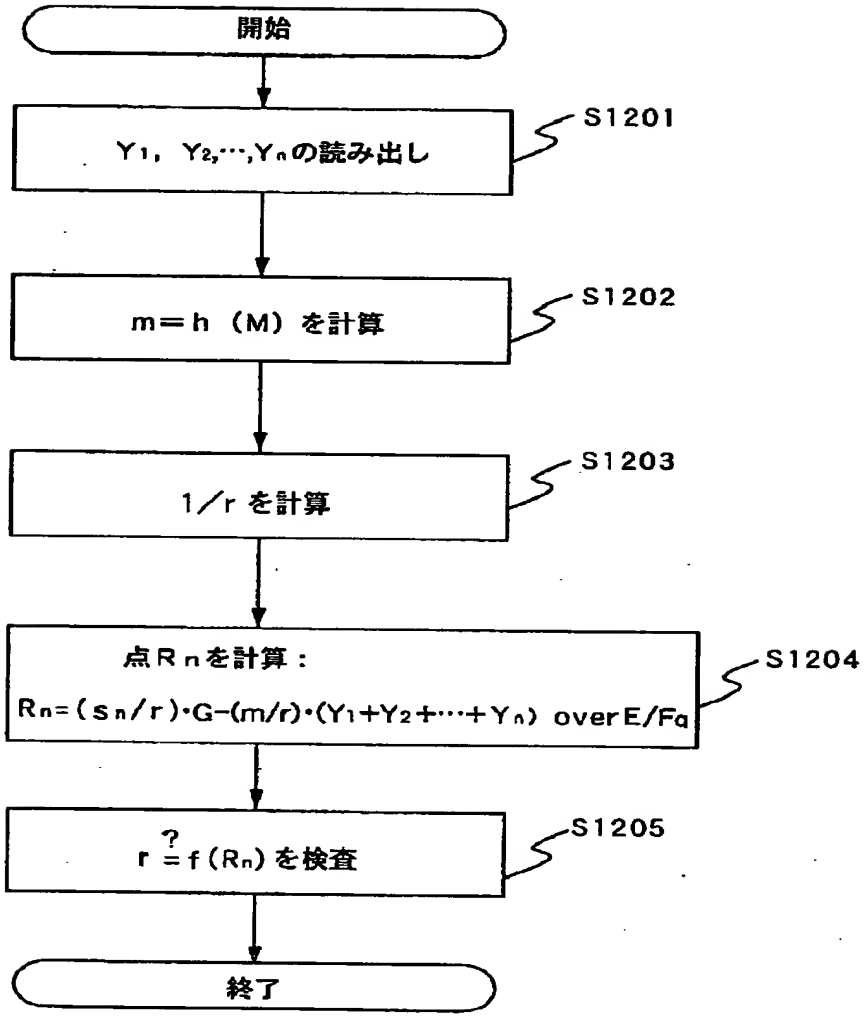
【図６】


開始
Y1, Y2,…,Yn の読み出し
S401
多重署名の検査:
m＝h (M) を計算
r＝f (Rn) を計算
Sn・G≟m・(Y1+Y2+…+Yn)+r・Rn overE/Fq
S402
終了

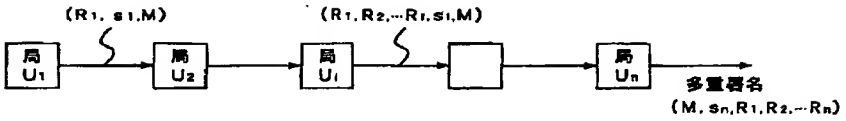
【図５】


(a)
開始
S301
乱数ki生成
S302
Ri計算：
Ri=Ri-1+ki・G over E/Fq
S303
Ri, Mの送信
終了
(b)
開始
S304
Y1, Y2,…,Yi-1の読み出し
S305
部分署名Si-1の検査：
m=h(M) を計算、
si-1・G=m・(Y1+Y2+…+Yi-1)+r・Ri-1 over E/Fq
S306
検査OK？
NO
YES
S307
si 計算
si=Si-1+xi・m+ki・r (mod Z)
S308
si, rの送信
終了

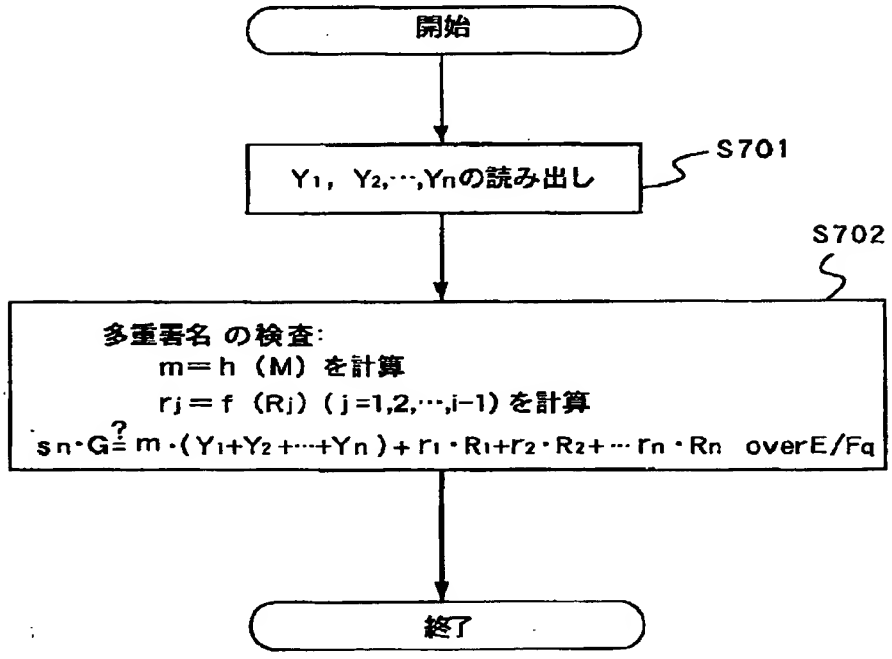
【図７】


開始
Y1，Y2,…,Ynの読み出し
S1201
m＝h（M）を計算
S1202
1／r を計算
S1203
点Rnを計算：
Rn=(sn/r)･G-(m/r)･(Y1+Y2+…+Yn) overE/Fa
S1204
r ?= f(Rn) を検査
S1205
終了

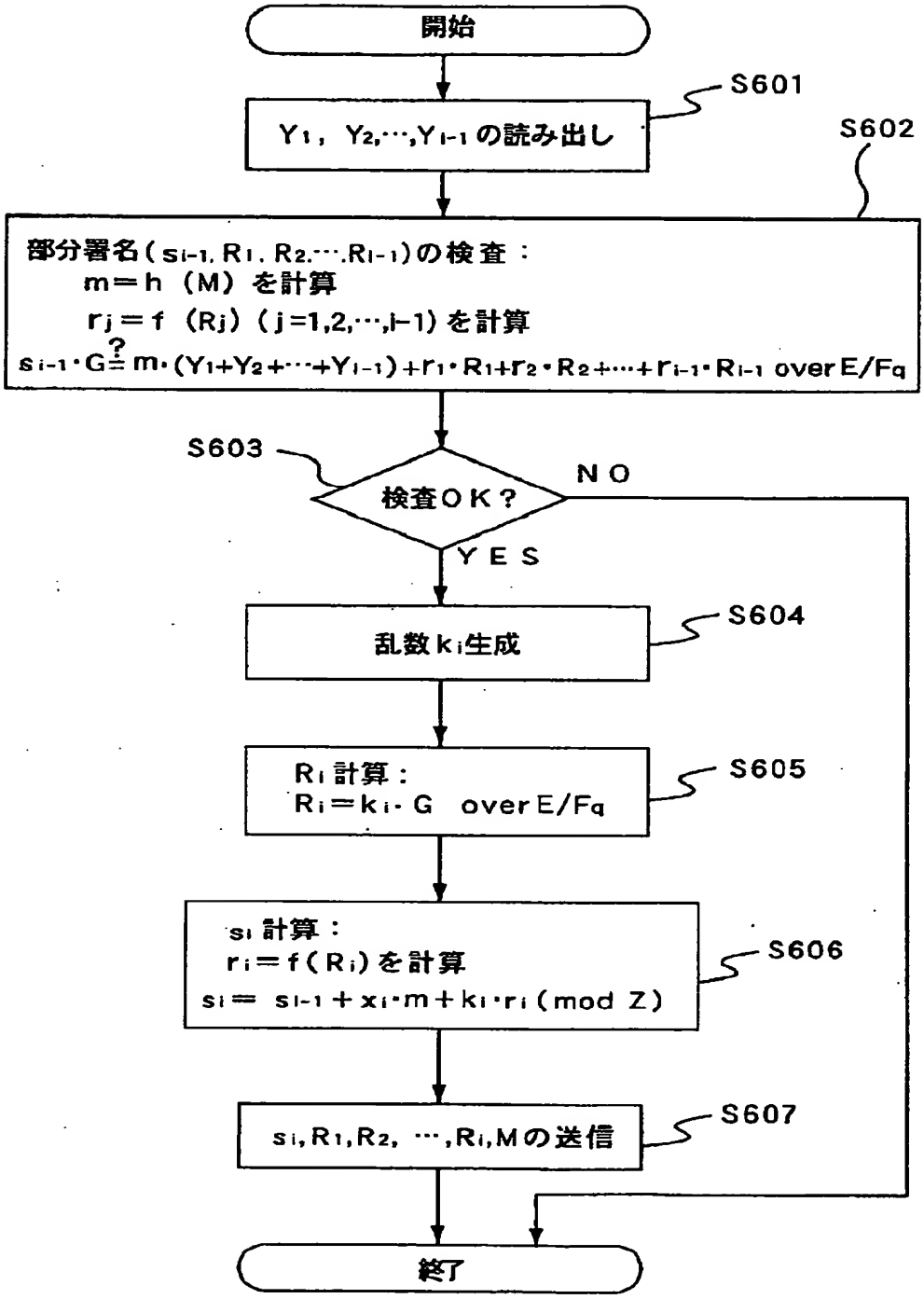
【図８】


(R1, s1,M)
(R1,R2,…Ri,si,M)
局 U1
局 U2
局 Ui
局 Un
多重署名
(M, sn,R1,R2,…Rn)

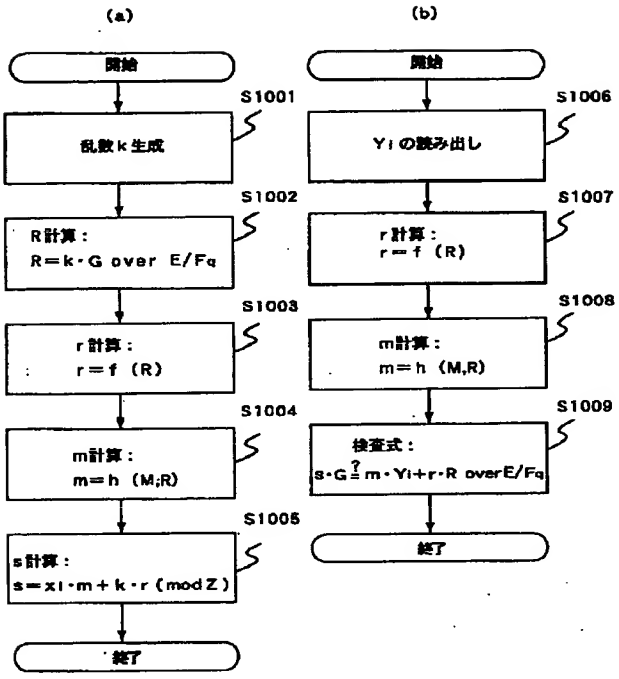
【図１０】


開始
Y1, Y2,…,Ynの読み出し
S701
S702
多重署名 の検査:
m＝h（M）を計算
rj＝f（Rj）（j=1,2,…,i−1）を計算
sn・G ? m・(Y1+Y2+…+Yn)+r1・R1+r2・R2+…rn・Rn overE/Fq
終了

【図９】


開始
S601
Y_1, Y_2,…,Y_{i-1} の読み出し
S602
部分署名(s_{i-1}, R_1, R_2,…,R_{i-1})の検査：
m＝h（M）を計算
r_j＝f（R_j）（j=1,2,…,i-1）を計算
$s_{i-1}\cdot G \stackrel{?}{=} m\cdot(Y_1+Y_2+\cdots+Y_{i-1})+r_1\cdot R_1+r_2\cdot R_2+\cdots+r_{i-1}\cdot R_{i-1}$ over E/Fq
S603
検査ＯＫ？
ＮＯ
ＹＥＳ
S604
乱数k_i生成
S605
R_i計算：
$R_i=k_i\cdot G$ over E/Fq
S606
s_i計算：
r_i＝f(R_i)を計算
$s_i=s_{i-1}+x_i\cdot m+k_i\cdot r_i$ (mod Z)
S607
s_i,R_1,R_2, …,R_i,Mの送信
終了

【図１２】


(a)
開始
S1001
乱数ｋ生成
S1002
R計算：
R＝k･G over E/Fq
S1003
r計算：
r＝f（R）
S1004
m計算：
m＝h（M,R）
S1005
s計算：
s＝x1･m＋k･r（mod Z）
終了
(b)
開始
S1006
Yiの読み出し
S1007
r計算：
r＝f（R）
S1008
m計算：
m＝h（M,R）
S1009
検査式：
s･G ? m･Yi＋r･R overE/Fq
終了